Advisory Alert

Alert Number: **AAA20221212** **Date:** **December 12, 2022**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**High**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31696, CVE-2022-31697, CVE-2022-31698, CVE-2022-31699)
Description	VMware has released security updates addressing multiple vulnerabilities that exist in their products **CVE-2022-31696** – A memory Corruption vulnerability exists in VMware ESXi because of the way it handles the network socket. A malicious actor with local access to ESXi may exploit this issue to corrupt memory leading to an escape of the ESXi sandbox. **CVE-2022-31697** – An Information disclosure vulnerability exists in vCenter Server due to the logging of credentials in plaintext. Using this vulnerability, a malicious actor with access to a workstation that invoked a vCenter Server Appliance ISO operation (Install/Upgrade/Migrate/Restore) can access plaintext passwords used during that operation. **CVE-2022-31698 –** A denial of service vulnerability exists in VMware vCenter server content library service. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to trigger a denial-of-service condition by sending a specially crafted header. **CVE-2022-31699 -** A heap-overflow vulnerability exists in VMware ESXi. Using this vulnerability a malicious local actor with restricted privileges within a sandbox process may exploit this issue to achieve a partial information disclosure. VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware ESXi version 6.5, 6.7, 7.0 VMware vCenter Server version 6.5, 6.7, 7.0 Cloud Foundation (vCenter Server) version 4x, 3x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0030.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.